PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-026899
(43)Date of publication of application : 25.01.2002

(51)Int.Cl. H04L 9/32
G09C 1/00
H04B 7/24
H04Q 7/38
H04L 12/28

(21)Application number : 2000-184697
(22)Date of filing : 20.06.2000

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : NOGUCHI TETSUYA
SHIMOTOONO SUSUMU

(54) VERIFICATION SYSTEM FOR AD HOC WIRELESS COMMUNICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a verification system for ad hoc wireless communication that can simply verify data integrity in data transmission reception by ad hoc wireless connection.
SOLUTION: A request source and a request destination for opening an encryption communication path are respectively defined to be a transmission source A and a transmission destination B. A verification data generating algorithm ID 1 is arranged in advance between the parties A, B. The A transmits e.g. a public key Kp of the A to the B, generates verification data Xp from the public key Kp by using the algorithm ID 1 and outputs the data to its own verification image display section 27. The B receives the data Kx sent from the A as the key Kp, generates verification data Xx from the Kx by using the ID 1 and outputs the data to its own verification image display section 27. A verifier discriminates that there exists data integrity when the Xp, Xx of the verification image display sections 27 of the parties A, B are coincident.

LEGAL STATUS

[Date of request for examination]	09.05.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3552648
[Date of registration]	14.05.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] The data for identity data generation to another side from one side of two data transmission-and-reception equipments mutually connected by ad hoc wireless connection with delivery and one data transmission-and-reception equipment The identity data generated based on the 1st generation algorithm from the transmitted data for identity data generation is made to output to one's identity data output section. With the data transmission-and-reception equipment of another side The identity data generated based on said 1st generation algorithm from the received data for identity data generation is made to output to one's identity data output section. The verification system for ad hoc radio characterized by judging whether the identity data in the identity data output section of both data transmission-and-reception equipment is mutually in agreement.

[Claim 2] Said identity data is a verification system for ad hoc radio according to claim 1 characterized by being visual or acoustic-sense-identity data.

[Claim 3] Identity data is a verification system for ad hoc radio according to claim 1 characterized by being outputted with the output gestalt of visual and acoustic-sense-both in the detection data output section.

[Claim 4] The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as

the output of this operator. The same or the serial operator train which arranged in one or more pieces and a serial a different operator which starts a tropism function on the other hand is established. The verification system for ad hoc radio according to claim 1 to 3 characterized by using the input of this serial operator train as the data for identity data generation, and using the output or its correspondence value of this serial operator train as identity data.

[Claim 5] Said 1st generation algorithm is a verification system for ad hoc radio according to claim 1 to 3 characterized by judging whether two or more identity data is generated and the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.

[Claim 6] The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as the output of this operator. The same or the serial operator train which arranged in two or more pieces and a serial a different operator which starts a tropism function on the other hand is established. Use the input of this serial operator train as the data for identity data generation, and the output of two or more operators chosen from all the operators that constitute this serial operator train, or its correspondence value is used as identity data, respectively. The verification system for ad hoc radio according to claim 5 characterized by judging whether the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.

[Claim 7] The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as the output of this operator. Prepare two or more mutually different operators which start a tropism function on the other hand, and the data for identity data generation are considered as the common input of each operator. The verification system for ad hoc radio according to claim 5 which uses the output or its correspondence value of each operator as identity data, respectively, and is characterized by judging whether the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.

[Claim 8] Said data for identity data generation are a verification system for ad hoc radio according to claim 1 to 7 characterized by being the public key of one data transmission-and-reception equipment.

[Claim 9] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function by said ad hoc radio verification system to the personal digital assistant with a radio function of the user of another side is verified A public key Kp

is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user. The personal computer with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal computer with a radio function Based on the information transmitted using the code by the public key from the personal computer with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. The personal computer with both the radio function is a data transmission-and-reception system for ad hoc radio using the verification system for ad hoc radio according to claim 8 characterized by sending and receiving data in the code based on the common key Kc henceforth.

[Claim 10] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function by said ad hoc radio verification system to the personal digital assistant with a radio function of the user of another side is verified The personal digital assistant with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal digital assistant with a radio function Based on the information transmitted using the code by the public key from the personal digital assistant with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. The common key Kc is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user. Next, the personal computer with both the radio function Henceforth, the data transmission-and-reception system for ad hoc radio using the verification system for ad hoc radio according to claim 8 characterized by sending and receiving data in the code based on the common key Kc.

[Claim 11] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function to the personal digital assistant with a radio function of the user of another side is verified A public key Kp is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user. The personal computer with a radio function of the user of another side The common key Kc is generated based on the 2nd generation algorithm from a public key Kp. One user's personal computer with a radio function Based on the information transmitted using the code by the public key from the personal computer with a radio function of the user of another side, the common key Kc is generated from the 2nd generation

algorithm. The personal computer with both the radio function is a data transmission-and-reception system for ad hoc radio characterized by sending and receiving data in the code based on the common key Kc henceforth.

[Claim 12] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function to the personal digital assistant with a radio function of the user of another side is verified The personal digital assistant with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal digital assistant with a radio function Based on the information transmitted using the code by the public key from the personal digital assistant with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. Next, the common key Kc is a data transmission-and-reception system for ad hoc radio which is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user, and is characterized by the personal computer with both the radio function sending and receiving data in the code based on the common key Kc henceforth.

[Claim 13] The data for identity data generation to another side from one side of two data transmission-and-reception equipments mutually connected by ad hoc wireless connection with delivery and one data transmission-and-reception equipment The identity data generated based on the 1st generation algorithm from the transmitted data for identity data generation is made to output to one's identity data output section. With the data transmission-and-reception equipment of another side The identity data generated based on said 1st generation algorithm from the received data for identity data generation is made to output to one's identity data output section. The verification approach for ad hoc radio characterized by judging whether the identity data in the identity data output section of both data transmission-and-reception equipment is mutually in agreement.

[Claim 14] Said identity data is the verification approach for ad hoc radio according to claim 13 characterized by being visual or acoustic-sense-identity data.

[Claim 15] Identity data is the verification approach for ad hoc radio according to claim 13 characterized by being outputted with the output gestalt of visual and acoustic-sense-both in the detection data output section.

[Claim 16] The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as the output of this operator. The same or the serial operator train which arranged in one or more pieces and a serial a different operator which starts a tropism function on the other hand is established. The verification approach for ad hoc radio according

to claim 13 to 15 characterized by using the input of this serial operator train as the data for identity data generation, and using the output or its correspondence value of this serial operator train as identity data.
[Claim 17] Said 1st generation algorithm is the verification approach for ad hoc radio according to claim 13 to 15 characterized by judging whether two or more identity data is generated and the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.
[Claim 18] The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as the output of this operator. The same or the serial operator train which arranged in two or more pieces and a serial a different operator which starts a tropism function on the other hand is established. Use the input of this serial operator train as the data for identity data generation, and the output of two or more operators chosen from all the operators that constitute this serial operator train, or its correspondence value is used as identity data, respectively. The verification approach for ad hoc radio according to claim 17 characterized by judging whether the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.
[Claim 19] The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as the output of this operator. Prepare two or more mutually different operators which start a tropism function on the other hand, and the data for identity data generation are considered as the common input of each operator. The verification approach for ad hoc radio according to claim 17 which uses the output or its correspondence value of each operator as identity data, respectively, and is characterized by judging whether the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.
[Claim 20] Said data for identity data generation are the verification approach for ad hoc radio according to claim 13 to 19 characterized by being the public key of one data transmission-and-reception equipment.
[Claim 21] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function by said ad hoc radio verification system to the personal digital assistant with a radio function of the user of another side is verified A public key Kp is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user. The personal computer with a radio

function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal computer with a radio function Based on the information transmitted using the code by the public key from the personal computer with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. The personal computer with both the radio function is the data transmission-and-reception approach for ad hoc radio of using the verification approach for ad hoc radio according to claim 20 characterized by sending and receiving data in the code based on the common key Kc, henceforth.
[Claim 22] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function by said ad hoc radio verification system to the personal digital assistant with a radio function of the user of another side is verified The personal digital assistant with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal digital assistant with a radio function Based on the information transmitted using the code by the public key from the personal digital assistant with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. The common key Kc is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user. Next, the personal computer with both the radio function Henceforth, the data transmission-and-reception approach for ad hoc radio of using the verification approach for ad hoc radio according to claim 20 characterized by sending and receiving data in the code based on the common key Kc.
[Claim 23] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function to the personal digital assistant with a radio function of the user of another side is verified A public key Kp is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user. The personal computer with a radio function of the user of another side The common key Kc is generated based on the 2nd generation algorithm from a public key Kp. One user's personal computer with a radio function Based on the information transmitted using the code by the public key from the personal computer with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. The personal computer with both the radio function is the data transmission-and-reception approach for ad hoc radio characterized by sending and

receiving data in the code based on the common key Kc henceforth.
[Claim 24] The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function to the personal digital assistant with a radio function of the user of another side is verified The personal digital assistant with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal digital assistant with a radio function Based on the information transmitted using the code by the public key from the personal digital assistant with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. Next, the common key Kc is the data transmission-and-reception approach for ad hoc radio which is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user, and is characterized by the personal computer with both the radio function sending and receiving data in the code based on the common key Kc henceforth.
[Claim 25] The record medium which recorded the program for verification systems of the following contents for ad hoc radio.
The data for identity data generation to another side from one side of two data transmission-and-reception equipments mutually connected by ad hoc wireless connection : With delivery and one data transmission-and-reception equipment The identity data generated based on the 1st generation algorithm from the transmitted data for identity data generation is made to output to one's identity data output section. With the data transmission-and-reception equipment of another side The identity data generated based on said 1st generation algorithm from the received data for identity data generation is made to output to one's identity data output section, and it is judged whether the identity data in the identity data output section of both data transmission-and-reception equipment is mutually in agreement.
[Claim 26] The record medium according to claim 25 which recorded the program for verification systems of the following contents for ad hoc radio.
: Said identity data is visual or acoustic-sense-identity data.
[Claim 27] The record medium according to claim 25 which recorded the program for verification systems of the following contents for ad hoc radio.
: Identity data is outputted with the output gestalt of visual and acoustic-sense-both in the detection data output section.
[Claim 28] The record medium according to claim 25 to 27 which recorded the program for verification systems of the following contents for ad hoc radio.
: The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as the

output of this operator, and the same or the serial operator train which arranged in one or more pieces and a serial a different operator which starts a tropism function on the other hand is established, use the input of this serial operator train as the data for identity data generation, and let the output or its correspondence value of this serial operator train be identity data.
[Claim 29] The record medium according to claim 25 to 27 which recorded the program for verification systems of the following contents for ad hoc radio.
: It is judged whether said 1st generation algorithm generates two or more identity data, and its things in the identity data output section of both data transmission-and-reception equipment correspond mutually about each identity data.
[Claim 30] Distribution equipment which distributes the program for verification systems of the following contents for ad hoc radio.
The data for identity data generation to another side from one side of two data transmission-and-reception equipments mutually connected by ad hoc wireless connection : With delivery and one data transmission-and-reception equipment The identity data generated based on the 1st generation algorithm from the transmitted data for identity data generation is made to output to one's identity data output section. With the data transmission-and-reception equipment of another side The identity data generated based on said 1st generation algorithm from the received data for identity data generation is made to output to one's identity data output section, and it is judged whether the identity data in the identity data output section of both data transmission-and-reception equipment is mutually in agreement.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the verification system for ad hoc radio coping with the alteration of transmission data, the data transmission-and-reception system for ad hoc radio, the verification approach for ad hoc radio, the data transmission-and-reception approach for ad hoc radio, the record medium that recorded the program of correspondence on the list and that is reached and distributed, and distribution equipment.
[0002]
[Description of the Prior Art] When two unspecified persons transmit without a holder in bad faith altering data in the temporary short-distance radio which does not use a specific infrastructure like ad hoc radio, it is necessary to share the cryptographic key which is not in being known by the holder in bad faith. However, the method of

setting up the value which serves as a radical of the cryptographic key at any time at the time of a communication link is complicated, and especially the thing for which communications partners exchange [a communications partner] cryptographic keys by oral, a memorandum, etc. under situations, such as the first meeting, is almost impractical. There is an approach share a public key first, and the public key enciphers and shares a cryptographic key as an approach of sharing a cryptographic key automatically. However, there is a risk of the Mann Inn THE middle attack (Man-in-the-middle attack: please refer to p.48 to p.50 of the title:application cryptography (APPLIED CRYPTOGRAPHY) of author blues SHUNAIA (BRUCE SCHNEIER) of John Willie - and - Suns firm (John Wiley & Sons, Inc) publication about the detail of the Mann Inn THE middle attack.).

[0003] The outline of the risk of the data alteration in the Mann Inn THE middle attack is carried out. Drawing 1 shows the room to which holder-in-bad-faith C intervenes among both while the transmission place B has not noticed the transmitting agency A in the ad hoc radio communications system 10. If, as for A and B, direct and a channel are established among both as shown in (a), even if it considers, as shown in (b), in fact, the third person may be wedging himself among both. "Man-in-the-Middle Attack" mentions concretely how it performs, and explains an example.

[0004] The general procedure of wireless cryptocommunication way establishment is as follows.

Procedure 1: Appeal for a transmitting agency toward many and unspecified partners by ID of the transmission place which wants to communicate.

Procedure 2: If a transmission place is in the range in which wireless connection is possible, the ID (that is, its ID) for which it appealed will be received.

Procedure 3: A transmission place tells a self operating condition etc. to a transmitting agency.

Procedure 4: Determine parameters [required for channel establishment] (selection of the channel to be used, a setup, exchange of a cryptographic key, etc.) of operation in both.

Procedure 5: Channel establishment is carried out and two-way communication is started.

[0005] What a holder in bad faith tends to enter the location of C of drawing 1 to is timing to which two persons set as the object of tapping start radio by confrontation. That is, it intervenes in the procedures 1-3 in which the above was enumerated. Drawing 2 and drawing 3 show an example of a means for a holder in bad faith to enter the location of C of drawing 1 . The transmitting agency A obtains an appeal colander by Specification ID for no surrounding transmission place candidates on the character of an electric wave (procedure 1). Since the appeal in its ID can be heard (procedure 2), the transmission place B answers the transmitting agency A (procedure 3). Here, a holder in bad faith is going to answer the appeal to ID other

than himself, or perform appeal by ID other than himself, and plan the following **********. First, holder-in-bad-faith C throws the noise of the same frequency band at the response of the transmission place B, and the transmitting agency A prevents from catching the response. At this time, since the transmission place B does not know the fact of that noise, it changes for the above-mentioned procedure 4, and is waiting for the session initiation in the procedure 4 from the transmitting agency A. Since the transmitting agency A is not in a procedure 4, the transmission place B returns to the condition of hearing the appeal of one's ID again after a time-out. On the other hand, since the response from the transmission place B is not obtained by the transmitting agency A, that for which it appeals by the ID again same after a time-out (procedure 1) is common. That is, the transmitting agency A and the transmission place B begin to take the synchronization of a mutual procedure, utterly, will notice the failure by each time-out, and will return to the original condition.
[0006] The transmitting agency A stands by according to the timing for which it appeals by the same ID again, and holder-in-bad-faith C stands by also according to the timing which the transmission place B begins to hear again that the appeal of its ID is further. Henceforth, it answers the appeal of the transmitting agency A with holder-in-bad-faith C in the disguise of the transmission place B, and it performs appeal at the transmission place B which began to hear the appeal of its ID on the contrary with it. [in the disguise of the transmitting agency A] Of course, holder-in-bad-faith C is preparing the capacity to change one's ID to any ID. since it is not the same time of day above that the transmitting agency A and the transmission place B return to the original condition since the synchronization of a mutual procedure shifts -- such two -- it can become completely and holder-in-bad-faith C can perform an action. It is because the time of day when the transmission place B begins to stand by in the following event the transmitting agency A, respectively differs primarily, the events set as the object of a time-out also differ, so the timeout periods itself differ.
[0007] this -- it becomes completely, and by machining, it thinks that the transmitting agency A had a normal response from the transmission place B of normal, changes together with holder-in-bad-faith C from the channel establishment procedure 4, i.e., a procedure, it thinks that the transmission place B is the appeal from the transmitting origin A of normal, and changes together with [it is the same with a channel establishment procedure, and] a third person C. If it progresses to the above-mentioned procedure 5, it will become possible to intercept in the form where holder-in-bad-faith C relays commo data in between [mutual], without being known by the carrier of Both A and B device currently regarded as having secured the channel only by two persons. this -- becoming completely (junction) -- if it uses, C can alter the public key which A should send to B, for example, and it can substitute for the public key corresponding to the private key which C prepared beforehand secretly. By this, the cryptocommunication way originally built between A and B becomes effective only between A and C, and it becomes the cryptocommunication

way which C set up independently between C and B. That is, the encryption data sent from A are decrypted by C, and again, another encryption is applied for the encryption channels between C and B to them, and they are transmitted to it. The same is said of the reverse transmission. Having established the encryption channel with normal procedures, both A and B are a public key's being substituted secretly on the way, and not noticing the substitution, and bring a result intercepted. Such an attack (tapping depended for becoming completely) is called Man-in-the-middle attack. Since the encryption channel itself is safe, it becomes important [ensuring whether both who communicate are sharing the really same public key as dealing with such an attack].

[0008]

[Problem(s) to be Solved by the Invention] As a method of coping with Man-in-the-middle attack, expressing the individuals ID (usually a partner's identifier etc.) indicated in the certificate as a transmitting agency and a transmission place, and carrying out a visual comparison is also considered using the certificate which a certificate authority publishes. However, cost starts issue of a certificate at this. Moreover, when using a certificate authority, in order to attest by registering an identity, its identity will be opened to a communications partner and the problem that anonymity cannot be maintained also exists. Furthermore, when using the service which specifies a user from a public key like a yellow page (Yellow Page), the secure network connection by the telephone line etc. is required, and transaction cost starts.

[0009] The purpose of this invention is offering the verification system for ad-hoc radio which can prevent effectively the alteration of the data based on spoofing to a communications partner, the data transmission-and-reception system for ad-hoc radio, the verification approach for ad-hoc radio, the data transmission-and-reception approach for ad-hoc radio, the record medium that recorded the program of correspondence on a list and that reach and distribute, and distribution equipment, when sending and receiving data between the data transmission-and-reception equipment mutually connected by ad-hoc wireless connection. Other purposes of this invention are offering the verification system for ad-hoc radio which can omit an exchange of the password by oral or memorandum writing, and cannot use the certificate authority which does identity public presentation, but can verify a communications partner efficiently, smoothly, and correctly, the data transmission-and-reception system for ad-hoc radio, the verification approach for ad-hoc radio, the data transmission-and-reception approach for ad-hoc radio, the record medium that recorded the program of correspondence on a list and that reach and distribute, and distribution equipment.

[0010]

[Means for Solving the Problem] According to the verification system for ad hoc radio and approach of this invention, the data for identity data generation to another side from one side of two data transmission-and-reception equipments mutually

connected by ad hoc wireless connection Delivery, The identity data generated with one data transmission-and-reception equipment based on the 1st generation algorithm from the transmitted data for identity data generation is made to output to one's identity data output section. Moreover, the identity data generated with the data transmission-and-reception equipment of another side based on the 1st generation algorithm from the received data for identity data generation is made to output to one's identity data output section. It is judged whether the identity data in the identity data output section of both data transmission-and-reception equipment is mutually in agreement.

[0011] Since the distance of both data transmission-and-reception equipment needs to contrast the identity data in the identity data output section of both data transmission-and-reception equipment mutually, it is less than 10 etc.m with which a user (user) can keep company between both data transmission-and-reception equipment in several seconds typically, and is several m preferably. Suppose at the identity data generated based on the data for identity data generation that you may be the data for identity data generation itself. Identity data is set as what the judgment with the identity data mutually in agreement in the detection data output section of both data transmission-and-reception equipment tends to perform. If the software for verification started in both data transmission-and-reception equipment is generally the same, the generation algorithm same for generation of identity data will be used from the data for identity data generation. However, the user of both data transmission-and-reception equipment fixes suitably one in two or more generation algorithms on the spot.

[0012] One data transmission-and-reception equipment generates identity data based on the 1st generation algorithm from the transmitted data for identity data generation. The data transmission-and-reception equipment of another side generates identity data based on the 1st generation algorithm from the received data for identity data generation. And it means that being correctly transmitted to the data transmission-and-reception equipment of another side from one data transmission-and-reception equipment, i.e., a data integrity, was verified, without judging whether the identity data outputted from the detection data output section of both data transmission-and-reception equipment is in agreement, and altering the data for identity data generation on the way, if in agreement. Thus, a data integrity is efficiently verifiable.

[0013] According to the verification system for ad hoc radio and approach of this invention, identity data is visual or acoustic-sense-identity data.

[0014] An image, a numeric value, alphabetic characters, or those combination are in visual identity data. As an example of a vision display of identity data, when identity data is a total of n-bit bit data, n bits is classified by every [a bit, such as continuing,], and there is a histogram which makes as a partition in the direction of a x axis, and is made into the quantity for every partition in the direction of the y-axis. As an example of an acoustic-sense display of identity data, the sound of the height

corresponding to the quantity of each partition of the above-mentioned histogram is outputted in an order from the partition of lower order. As for identity data, it is desirable that that a user tends to judge smoothly and correctly the coincidence of identity data and the inequality in both data transmission-and-reception equipment to be is chosen.

[0015] According to the verification system for ad hoc radio and approach of this invention, identity data should be outputted with the output gestalt of visual and acoustic-sense-both in the detection data output section.

[0016] With the visual output gestalt of identity data, even if the things in both data transmission-and-reception equipment are similar, in the acoustic-sense-output gestalt of identity data, a difference is clear or that case of being reverse exists. The accuracy of a judgment of coincidence and an inequality increases by contrasting both the visual output gestalt of identity data, and an acoustic-sense-output gestalt.

[0017] According to the verification system for ad hoc radio and approach of this invention, a function A operator, The input of this operator and the result of an operation of this operator are defined for the numeric value on which this operator acts as the output of this operator. The same or the serial operator train which arranged in one or more pieces and a serial a different operator which starts a tropism function on the other hand is established, use the input of this serial operator train as the data for identity data generation, and let the output or its correspondence value of this serial operator train be identity data.

[0018] On the other hand, there is a Hash Function (Hash Function) in a tropism function. The operator also contains the thing only with one piece in the operator train which carried out [above-mentioned] the definition. By on the other hand making a tropism function participate in generation of the identity data from the data for identity data generation, the difficulty which finds out the data for identity data generation from identity data increases, and possibility that a holder in bad faith will do a data alteration using the data for identity data generation of a false similar to the true data for identity data generation falls. In addition, the more serial arithmetic child queue length becomes long, the more it becomes impossible in computational complexity to find out the data for identity data generation from identity data.

[0019] According to the verification system for ad hoc radio and approach of this invention, it is judged whether the 1st generation algorithm generates two or more identity data, and its things in the identity data output section of both data transmission-and-reception equipment correspond mutually about each identity data.

[0020] Possibility that two or more identity data of all is similar is very low. The accuracy of verification improves by generating two or more identity data and judging whether the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.

[0021] According to the verification system for ad hoc radio and approach of this invention, a function A operator, The input of this operator and the result of an

operation of this operator are defined for the numeric value on which this operator acts as the output of this operator. The same or the serial operator train which arranged in two or more pieces and a serial a different operator which starts a tropism function on the other hand is established. Use the input of this serial operator train as the data for identity data generation, and the output of two or more operators chosen from all the operators that constitute this serial operator train, or its correspondence value is used as identity data, respectively. It is judged whether about each identity data, the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement.

[0022] According to the verification system for ad hoc radio and approach of this invention, a function A operator, The input of this operator and the result of an operation of this operator are defined for the numeric value on which this operator acts as the output of this operator. Prepare two or more mutually different operators which start a tropism function on the other hand, and the data for identity data generation are considered as the common input of each operator. The output or its correspondence value of each operator is used as identity data, respectively, and it is judged whether the things in the identity data output section of both data transmission-and-reception equipment are mutually in agreement about each identity data.

[0023] According to the verification system for ad hoc radio and approach of this invention, the data for identity data generation are the public key of one data transmission-and-reception equipment.

[0024] If the data for identity data generation are the public key of one data transmission-and-reception equipment, it is verifiable that the public key which the data transmission-and-reception equipment of another side received is a public key of one data transmission-and-reception equipment with verification of identity data. Therefore, it carries out sending a common key etc. to one data transmission-and-reception equipment from the data transmission-and-reception equipment of another side by the cryptocommunication using the public key of one data transmission-and-reception equipment etc., and cryptocommunication with the common key between both data transmission-and-reception equipment can be established completely.

[0025] According to the data transmission-and-reception system for ad hoc radio and approach of this invention of using the above-mentioned verification system for ad hoc radio The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function by the ad hoc radio verification system to the personal digital assistant with a radio function of the user of another side is verified A public key Kp is transmitted to a personal computer with a radio function from a personal digital

assistant with a radio function in each user. The personal computer with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal computer with a radio function Based on the information transmitted using the code by the public key from the personal computer with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm, and data are henceforth sent [the personal computer with both the radio function] and received in the code based on the common key Kc.

[0026] According to the data transmission-and-reception system for ad hoc radio and approach of this invention of using the above-mentioned verification system for ad hoc radio The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function by the ad hoc radio verification system to the personal digital assistant with a radio function of the user of another side is verified The personal digital assistant with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal digital assistant with a radio function Based on the information transmitted using the code by the public key from the personal digital assistant with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. Next, data are henceforth sent [the common key Kc is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user, and / the personal computer with both the radio function] and received in the code based on the common key Kc.

[0027] According to the data transmission-and-reception system for ad hoc radio and approach of this invention The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function to the personal digital assistant with a radio function of the user of another side is verified A public key Kp is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user. The personal computer with a radio function of the user of another side The common key Kc is generated based on the 2nd generation algorithm from a public key Kp. One user's personal computer with a radio function Based on the information transmitted using the code by the public key from the personal computer with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm, and data are henceforth sent [the personal computer with both the radio

function] and received in the code based on the common key Kc.
[0028] According to the data transmission-and-reception system for ad hoc radio and approach of this invention The personal digital assistant with a radio function and the personal computer with a radio function which are owned by each user exist. It is connected with the channel with secure each user's personal digital assistant with a radio function and personal computer with a radio function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a radio function to the personal digital assistant with a radio function of the user of another side is verified The personal digital assistant with a radio function of the user of another side The common key Kc is generated from the 2nd generation algorithm. One user's personal digital assistant with a radio function Based on the information transmitted using the code by the public key from the personal digital assistant with a radio function of the user of another side, the common key Kc is generated from the 2nd generation algorithm. Next, data are henceforth sent [the common key Kc is transmitted to a personal computer with a radio function from a personal digital assistant with a radio function in each user, and / the personal computer with both the radio function] and received in the code based on the common key Kc.
[0029] The secure channel of each user's personal digital assistant with a radio function and a personal computer with a radio function is established by the two-way communication by for example, each user's private key. The personal digital assistant with a radio function contains what is called PDA (Personal Digital Assistant). Hiding computing (Hidden Computing: explain the gestalt of implementation of invention in full detail) as an example of the style of work of a businessman is considered. In hidden computing, transmission and reception of data are wanted to be performed, for example without an alteration in personal computers with a radio function, such as Note PC. If it is verified in such a case that the user was transmitted to the personal digital assistant with a radio function of another side, without altering the public key Kp of one personal digital assistant with a radio function on the way from contrast of the identity data in the identity data output section of a personal digital assistant with a radio function The verification is made to take over to both users' personal computer with a radio function, and cryptocommunication can be smoothly carried out with the common key Kc between personal computers with both the radio function.
[0030] The program which the record medium and distribution equipment of this invention record and distribute, respectively is the thing of the following contents. The data for identity data generation to another side from one side of two data transmission-and-reception equipments mutually connected by ad hoc wireless connection : With delivery and one data transmission-and-reception equipment The identity data generated based on the 1st generation algorithm from the transmitted data for identity data generation is made to output to one's identity data output section. With the data transmission-and-reception equipment of another side The

identity data generated based on the 1st generation algorithm from the received data for identity data generation is made to output to one's identity data output section, and it is judged whether the identity data in the identity data output section of both data transmission-and-reception equipment is mutually in agreement.

[0031] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further. ******.

: Identity data is visual or acoustic-sense-identity data.

[0032] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further.

: Identity data is outputted with the output gestalt of visual and acoustic-sense-both in the detection data output section.

[0033] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further.

: The input of this operator and the result of an operation of this operator are defined for the numeric value on which a operator and this operator act a function as the output of this operator, and the same or the serial operator train which arranged in one or more pieces and a serial a different operator which starts a tropism function on the other hand is established, use the input of this serial operator train as the data for identity data generation, and let the output or its correspondence value of this serial operator train be identity data.

[0034] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further.

: It is judged whether the 1st generation algorithm generates two or more identity data, and its things in the identity data output section of both data transmission-and-reception equipment correspond mutually about each identity data.

[0035]

[Embodiment of the Invention] Hereafter, the gestalt of implementation of invention is explained with reference to a drawing. Drawing 4 is the flow chart of the whole code data transmission following verification and it of a data integrity. A cryptocommunication open request side and a requestor side-ed are defined as a transmitting agency and a transmission place, respectively, and A and transmission place data transmission-and-reception equipment are set to B for transmitting agency data transmission-and-reception equipment in drawing 4 . the transmission origin of the public key for data-integrity verification and the transmission place, and the transmission origin of this transmission after data-integrity verification (code transmission using a ******** right [that]:common key) and a transmission place do not need to be in agreement, and may be reverse, and a transmitting agency and a

transmission place may interchange suitably in this transmission after data-integrity verification.

[0036] Processing of drawing 4 is explained in order.

(a) A transmits ID (this ID is hereafter called "ID1".) which specifies its public key Kp and identity data generation algorithm as B with a cryptocommunication way open request. A generates identity data Xp to coincidence based on its own public key Kp.

(b) B sets to Kx the data received as a public key Kp of A to A. If there is no alteration of data on the radio-transmission way from A to B, it will become Kx=Kp, and if there is an alteration, Kx will become what has another Kp. B generates identity data Xx with the identity data generation algorithm of ID1 with the assignment [A] with origin of Kx received from A. The example of identity data is explained in full detail in below-mentioned drawing 5 .

(c) The user of A and B verifies whether the identity data Xp and Xx by which it was indicated by the output, respectively is the same to the display of A and B. If it is Xp=Xx, a judgment that Kx=Kp is meant and there is a data integrity in the channel of A-B will be made.

(d) B enciphers ID (this ID is hereafter called "ID2".) which specifies the random-number value R and common key generation algorithm for common key generation using the public key Kp received from A, and transmits to A. About ID2, that A and B use the same communication software etc. can omit transmission between A-B like ID1, if ID2 is being fixed. B uses a common key generation algorithm for coincidence from the random-number value R, and generates the common key Kc.

(e) A decodes the enciphered random-number value R which was received from B using the private key corresponding to a public key Kp, acquires the random-number values R and ID2, and generates the common key Kc using the common key generation algorithm of ID2 from the random-number value R.

(f) A-B sends and receives data by the encryption communication link based on the common key Kc henceforth.

[0037] The identity data displayed on the identity data output section of A and B may be the data for identity data generation (for example, the public key of A itself) itself. That is, fatbits of the public key of A is carried out to the data for identity data generation of A and B. However, numerically, since it is hard to read, the digital readout of a public key may be changed into image display. Drawing 5 shows the histogram as an example of the identity data generated from the data for identity data generation. A vision indication of the identity data is given at the verification image display section 27 of data transmission-and-reception equipment 20 (drawing 6). Identity data is expressed in sequence to the area of the number of bits equal in from LSB to MSB in the public key by the histogram which makes a break and an axis of abscissa an area and makes an axis of ordinate the quantity of each area that the data for identity data generation are the public key of A. Since the data Kx for identity data generation which the public key Kp of A became completely by the

holder in bad faith in the middle of the transmission line, and B received from A when there was no **** crack **** are equal to the data Kp for identity data generation, they serve as Xx=Xp. Therefore, the user of A and/or B or other verification persons who can trust it If the display of A and B is seen directly, Xp and Xx which are displayed on the display of A and B are contrasted (comparison) and both are in agreement It judges that the public key of A has been transmitted to B as it is from A, namely, judges that there is a data integrity, and if both are inharmonious, it will be judged that there was an alteration of data in the middle of transmission to B from A.
[0038] However, the difference from the small similar public key of the Hamming DISU wardrobe of the precision of human being's recognition capacity may be undetectable only by generating the comparison image of a histogram like drawing 5 simply necessarily highly. Then, to a public key, on the other hand, a Hash Function etc. may change into predetermined data with the application of a tropism function, and may display verification images, such as a histogram, for it. in this case -- even if it is going to ask for another public key which outputs the data with which the third person who is going to perform ********** is similar -- dispersion -- a logarithm -- a problem will be solved and it is impossible in computational complexity. However, the amount of information of the verification image to create may be broken by exhaustive search, when very small compared with the bit size of a public key. Under such conditions, to the data which already applied the tropism function on the other hand, new data are computed, or, further on the other hand, new data are computed with the application of another one direction nature function to a public key with the application of a tropism function, and another verification image is generated. Two or more verification images can be generated and the reinforcement which receives becoming completely by using this can be raised with repeating this actuation.
[0039] Identity data is not limited to an image like a histogram, but may be shown to a user, and combining two or more of those data. [using the display of alphabetic data, change of a scale etc.] As acoustic-sense-identity data, the value of the direction of an axis of ordinate of the histogram of drawing 5 is made to correspond to the height or the tone of a sound, and the sound corresponding to the value of each area is outputted to sequence for every predetermined time from the area of Hidari of the direction of an axis of abscissa of drawing 6 . Moreover, you may make it make identity data output from both a vision drop and the loudspeaker as a sound emission means.
[0040] Drawing 6 - drawing 8 show the method which generates identity data from the data for identity data generation on the other hand using a tropism function, respectively. Data D1 mean the data for identity data generation, and data D2, D3, and D4 and ... mean identity data. Moreover, an one directivity each function functions as a operator, acts on an input, and outputs the result of an operation. On the other hand, a tropism function is a Hash Function (Hash Function).
[0041] In drawing 6 , a time, on the other hand, the 1st time makes the tropism

function F act on the data D1 as data for identity data generation, and data D2 are obtained. The loop formation which the tropism function F is made to act on them while it is the same to data D2, namely, contains the tropism function F on the other hand is formed, and the 2nd data D3 are obtained. Henceforth, loop-formation processing is repeated and D4, D5, and ... are obtained. After repeating the loop formation of the count of predetermined, the final result of an operation is set to Dn, this Dn is used as identity data, and this identity data is indicated by vision at the verification image display section 27 of data transmission-and-reception equipment 20 (drawing 10). It not only indicates by vision at the verification image display section 27 of data transmission-and-reception equipment 20, but only the final result of an operation Dn may make it make the verification image display section 27 of data transmission-and-reception equipment 20 indicate some of D2, D3, D4, specific ..., or all by vision by screen separation or time sharing, and you may contrast it about each which was displayed. Even if the judgment of the coincidence and the inequality about those one identity data is confusing by contrasting two or more identity data, possibility that the judgment of coincidence and an inequality will become confusing about two or more identity data of all contrasted is very small, and can improve the accuracy of the verification about a data alteration.

[0042] In addition, when D2, D3, D4, and ... all do not come out and it contrasts specific [some of], the protection reinforcement to a holder's in bad faith attack becomes high by changing the combination (Subset) about the some suitably.

[0043] plurality which is mutually different in drawing 7 -- on the other hand, prepare the tropism functions F, G, and H and ..., the one directivity each functions F, G, and H and ... are made to act on the common data D1, and each results of an operation D2, D3, and D4 and ... are obtained. It contrasts about each which the verification image display section 27 of data transmission-and-reception equipment 20 was made to indicate by vision, and was displayed on it by screen separation or time sharing by using some of D2, D3, D4, specific ..., or all as identity data.

[0044] In drawing 8 , two or more one side tropism functions F, G, and H and ... which are mutually different are prepared. A time, on the other hand, the 1st time makes the tropism function F act on the data D1 as data for identity data generation, and data D2 are obtained. A time, on the other hand, the 2nd time makes the tropism function G act on data D2, and data D3 are obtained. In this way, the one direction nature function of the next step is made to act on the result of an operation of the preceding paragraph one after another, and two or more D2, D3 and D4, and ... are obtained. It contrasts about each which the verification image display section 27 of data transmission-and-reception equipment 20 was made to indicate by vision, and was displayed on it by screen separation or time sharing by using some of D2, D3, D4, specific ..., or all as identity data. In addition, two or more methods of contrast can be considered to be the same special examples which used the tropism function F on the other hand in the method of drawing 8 instead of [in drawing 6 / mutually different]

on the other hand using a tropism function.
[0045] Drawing 9 is the block diagram showing the method which asks for identity data combining processing of drawing 6 – drawing 8 . The identity data computing type of drawing 6 – drawing 9 is defined as Types (Type) 1, 2, and 3, respectively. The data for identity data generation are inputted into the left end of drawing 8 , and identity data is outputted to the right end of drawing 8 . The example of an array of drawing 9 can choose two or more types from Types 1, 2, and 3 which are examples, can arrange them in order of arbitration, and can obtain the data for identity data generation.
[0046] Drawing 10 is the block diagram of data transmission–and–reception equipment 20. Since data transmission–and–reception equipment 20 becomes the transmitting agency A by the case, or became the transmission place B and is carried out, it combines the configuration as a transmitting agency, and the configuration as a transmission place. The public key of A which the transmission verification section 24 outputted its own public key to the verification image generation section 26 when data transmission–and–reception equipment 20 was A, and received as a transmitted and received data 31 from A in the communications department 25 when data transmission–and–reception equipment 20 was B is sent to the verification image generation section 26 via the transmission verification section 24. The verification image generation section 26 generates identity data from the public key which received from the transmission verification section 24, and the generated identity data is displayed on the verification image display section 27. Users, such as an owner of A and B, contrast the identity data in the verification image display section 27 of two data transmission–and–reception equipments 20 by which ad hoc wireless connection is made, investigate coincidence and an inequality, and input the result into the verification result input section 28. The input result to the verification result input section 28 from a user is notified to the transmission verification section 24, and it is judged that the transmission verification section 24 has a data integrity about the public key transmitted to B through the transmission line of ad hoc wireless connection from A when a notice that both identity data is mutually in agreement is received. Next, when data transmission–and–reception equipment 20 is B, a random–number value is generated in the random–number generation section 34, and the common key generation algorithm of ID2 generates a common key in the common key generation section 33 from the random–number value generated in the random–number generation section 34. On the other hand, the random–number value and ID2 which the random–number generation section 34 generated are enciphered based on the public key of A in decryption / encryption implementation section 32, and the code data Dc is sent to A through a transmitted and received data 31. Moreover, based on the generation algorithm of ID2, a common key is generated from the random–number value R, and it is saved in the key preservation section 35. When data transmission–and–reception equipment 20 is A, the transmitted and received data 31

of the code data Dc transmitted from B is decoded with its own private key in decryption / encryption implementation section 32, the random-number values R and ID2 are acquired, a common key is generated based on the common key generation algorithm of ID2 from the random-number value R, and this common key is saved in the key preservation section 35. Henceforth, when transmitting data, a common key is pulled out from the key preservation section 35, transmit data is enciphered in decryption / encryption implementation section 32 based on this common key, and it transmits to the other party as a transmitted and received data 31. When receiving data, it is received and enciphered and a transmitted and received data 31 is decoded in decryption / encryption implementation section 32, the Taira data are saved at a hard disk (not shown) etc., or predetermined processing is performed.

[0047] Drawing 11 is the flow chart of the communications processing by the side of the transmitting agency A. A public key Kp is transmitted (S40), the identity data generation algorithm of ID1 generates identity data Xp from this public key Kp (S42), and identity data Xp is outputted to the verification image display section 27 (S44). In S46, if their own identity data Xp and the identity data Xx of the transmission place B are contrasted and it is judged that it is the same, it will progress to S48, and if it is judged that it is inharmonious, this program will be ended as an error (a data integrity is not accepted). Although it progressed to S52 and the random-number value receiving latency time carried out predetermined time progress, when there was a data integrity and it judged that reception of the random-number value R from the transmission place B received the random-number value R in waiting (S48) and S50, when there is no reception of the random-number value R, this program is ended as an error. In S52, the code data of the random-number value R from the transmission place B are decoded with their private key, and the random-number value R is acquired. [of correspondence in said public key Kp] Between the data transmission-and-reception equipment of A and B, ID is beforehand fixed about two or more common key generation algorithms, respectively, and ID (an example ID2) adopted as this common key generation algorithm in the transmission place B has been transmitted to the transmitting agency A from the transmission place B together with the random-number value R. In this way, in S56, based on the common key generation algorithm of ID2, the common key for the communication link with the transmission place B is generated from the random-number value R, and B and an encryption communication link are henceforth started using this common key (S58).

[0048] Drawing 12 is the flow chart of the communications processing by the side of the transmission place B. A public key Kx is received from the transmitting agency A (S60). Since the holder in bad faith may intervene and may be altered by the transmission line between A and B, this received public key is made to express it as Kx instead of Kc. Next, the identity data generation algorithm specified by ID1 sent together with a public key Kp from the transmitting agency A generates identity data Xx from Kx (S62), and identity data Xx is outputted to the verification image display

section 27 (S64). In S66, if their own identity data Xx and the identity data Xp of the transmitting agency A are contrasted and it is judged that it is the same, it will progress to S68, and if it is judged that it is inharmonious, this program will be ended as an error (a data integrity is not accepted). When there is a data integrity, the random-number value R is generated (S68). The random-number value R The data which enciphered ID2 as ID of the selected common key generation algorithm with the public key of the transmitting agency A out of two or more common key generation algorithms this time are transmitted to the transmitting agency A (S70). The common key Kc is generated according to the common key generation algorithm of ID2 (S72), and A and an encryption communication link are henceforth started using this common key (S74).

[0049] Drawing 13 is an explanatory view which establishes the cryptocommunication way of ad hoc wireless connection among the users whom it hides and a computing style uses. It hides, and a user dedicates a computer to a bag etc. and computing (Hidden Computing) means the use gestalt which operates this computer by remote control using radio etc. from pocket devices, such as PDA (Personal Digital Assistant-ersonal Digital Assistant) at hand. 82 with which PDA80a etc. is equipped is a communication link device. [when performing ad hoc radio between the devices (notebook computers 88a and 88b in the = bags 86a and 86b) which have not equipped the system which can check the data integrity of a public key which was described above] A cryptocommunication way is indirectly established using PDA 80a and 80b which mounted these notebook computers 88a and 88b and the cryptocommunication way establishment protocol which has secured the secure channels 90a and 90b to beforehand. In addition, a channel secure [between PDA and a notebook computer] is attained by cryptocommunication with the common key fixed in advance for example, among both. In drawing 13 , a channel 84 is first established between PDA80a and 80b in a procedure (a), the public key of one PDA is transmitted to PDA of another side, and the data integrity of this public key is verified. Next, in a procedure (b), the data-integrity verification between PDA80a and 80b is inherited to the notebook computers 88a and 88b connected with each PDA 80a and 80b according to the secure channels 90a and 90b. Specifically, this succession is attained by transmitting notebook computers 88a and 88b through the secure channels 90a and 90b in the public key which had the data integrity verified between PDA80a and 80b. Henceforth, after sharing a common key through the channel 92 between both, data are sent [notebook computers 88a and 88b] and received in a code with this common key.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the room to which holder-in-bad-faith C intervenes among both while the transmission place B has not noticed the transmitting agency A.
[Drawing 2] It is drawing showing the 1st part of an example of a means for a holder in bad faith to enter the location of C of drawing 1 .
[Drawing 3] It is drawing showing the 2nd part of an example of a means for a holder in bad faith to enter the location of C of drawing 1 .
[Drawing 4] It is the flow chart of the whole code data transmission following verification and it of a data integrity.
[Drawing 5] It is drawing showing the histogram as an example of the identity data generated from the data for identity data generation.
[Drawing 6] It is drawing showing the 1st method which generates identity data from the data for identity data generation on the other hand using a tropism function.
[Drawing 7] It is drawing showing the 2nd method which generates identity data from the data for identity data generation on the other hand using a tropism function.
[Drawing 8] It is drawing showing the 3rd method which generates identity data from the data for identity data generation on the other hand using a tropism function.
[Drawing 9] It is the block diagram showing the method which asks for identity data combining processing of drawing 6 - drawing 8 .
[Drawing 10] It is the block diagram of data transmission-and-reception equipment.
[Drawing 11] It is the flow chart of the communications processing by the side of the transmitting agency A.
[Drawing 12] It is the flow chart of the communications processing by the side of the transmission place B.
[Drawing 13] It is the explanatory view which establishes the cryptocommunication way of ad hoc wireless connection among the users whom it hides and a computing style uses.
[Description of Notations]
10 Ad Hoc Radio Communications System
80a, 80b PDA (Personal Digital Assistant with a radio function)
88a, 88b Notebook computer (personal computer with a radio function)

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－26899
（P2002－26899A）
(43)公開日　平成14年１月25日(2002.1.25)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｂ　7/24	Ｅ	５Ｋ０３３
Ｈ０４Ｂ　7/24		Ｈ０４Ｌ　9/00	６７５Ｂ	５Ｋ０６７
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　9/00	６７１	

審査請求　有　　請求項の数30　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2000－184697(P2000－184697)

(22)出願日　平成12年６月20日(2000.6.20)

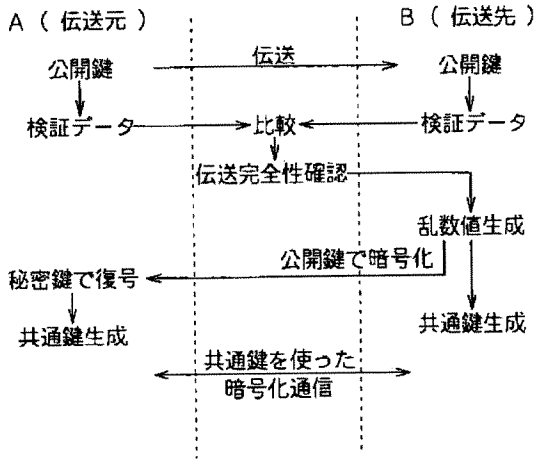
(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(74)復代理人　100085408
弁理士　山崎　隆　（外３名）

最終頁に続く

(54)【発明の名称】　アドホック無線通信用検証システム

(57)【要約】
【課題】　アドホック無線接続によるデータ送受信においてデータ完全性を簡単に検証する。
【解決手段】　暗号通信路開設を要求する要求元及び要求先をそれぞれ伝送元Ａ及び伝送先Ｂと定義する。ＡとＢとの間には、予め検証データ生成アルゴリズムＩＤ１が取り決められている。Ａは、Ｂへ例えばＡの公開鍵Ｋｐを伝送するとともに、ＩＤ１によりＫｐから検証データＸｐを生成し、それを自分の検証画像表示部２７へ出力する。Ｂは、ＡからＫｐとして伝送されて来たデータＫｘを受信し、ＩＤ１によりＫｘから検証データＸｘを生成し、それを自分の検証画像表示部２７へ出力する。検証者は、Ａ，Ｂの検証画像表示部２７のＸｐ，Ｘｘが一致しているならば、データ完全性があると判断する。



【特許請求の範囲】

【請求項１】　アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっていることを特徴とするアドホック無線通信用検証システム。

【請求項２】　前記検証データは、視覚的又は聴覚的な検証データであることを特徴とする請求項１記載のアドホック無線通信用検証システム。

【請求項３】　検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていることを特徴とする請求項１記載のアドホック無線通信用検証システム。

【請求項４】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされることを特徴とする請求項１～３のいずれかに記載のアドホック無線通信用検証システム。

【請求項５】　前記第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１～３のいずれかに記載のアドホック無線通信用検証システム。

【請求項６】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を２個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された２個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項５記載のアドホック無線通信用検証システム。

【請求項７】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項５記載のアドホック無線通信用検証システム。

【請求項８】　前記検証データ生成用データは一方のデータ送受装置の公開鍵であることを特徴とする請求項１～７のいずれかに記載のアドホック無線通信用検証システム。

【請求項９】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項８記載のアドホック無線通信用検証システムを利用するアドホック無線通信用データ送受システム。

【請求項１０】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項８記載のアドホック無線通信用検証システムを利用するアドホック無線通信用データ送受システム。

【請求項１１】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在

し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Ｋｐから共通鍵Ｋｃを第２の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受システム。

【請求項１２】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受システム。

【請求項１３】　アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっていることを特徴とするアドホック無線通信用検証方法。

【請求項１４】　前記検証データは、視覚的又は聴覚的な検証データであることを特徴とする請求項１３記載のアドホック無線通信用検証方法。

【請求項１５】　検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていることを特徴とする請求項１３記載のアドホック無線通信用検証方法。

【請求項１６】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされることを特徴とする請求項１３～１５のいずれかに記載のアドホック無線通信用検証方法。

【請求項１７】　前記第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１３～１５のいずれかに記載のアドホック無線通信用検証方法。

【請求項１８】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を２個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された２個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１７記載のアドホック無線通信用検証方法。

【請求項１９】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１７記載のアドホック無線通信用検証方法。

【請求項２０】　前記検証データ生成用データは一方のデータ送受装置の公開鍵であることを特徴とする請求項１３～１９のいずれかに記載のアドホック無線通信用検証方法。

【請求項２１】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公

開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項２０記載のアドホック無線通信用検証方法を利用するアドホック無線通信用データ送受方法。

【請求項２２】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項２０記載のアドホック無線通信用検証方法を利用するアドホック無線通信用データ送受方法。

【請求項２３】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Ｋｐから共通鍵Ｋｃを第２の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受方法。

【請求項２４】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受方法。

【請求項２５】　次の内容のアドホック無線通信用検証システム用プログラムを記録した記録媒体。

：アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【請求項２６】　次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項２５記載の記録媒体。

：前記検証データは、視覚的又は聴覚的な検証データである。

【請求項２７】　次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項２５記載の記録媒体。

：検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっている。

【請求項２８】　次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項２５～２７記載の記録媒体。

：関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【請求項２９】　次の内容のアドホック無線通信用検証

システム用プログラムを記録した請求項２５～２７記載の記録媒体。
：前記第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。
【請求項３０】　次の内容のアドホック無線通信用検証システム用プログラムを配信する配信装置。
：アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、伝送データの改ざんに対処するアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置に関するものである。
【０００２】
【従来の技術】アドホック無線通信のような特定のインフラを利用しないその場限りの近距離無線通信において不特定の二者が、データを悪意の第三者により改ざんされることなく、伝送する場合には、悪意の第三者に知られることにない暗号鍵を共有する必要がある。しかしながら、通信時に随時その暗号鍵の基となる値を設定する方法は煩雑であり、特に通信相手が初顔合わせ等の状況下では、通信相手同士が口頭やメモ等により暗号鍵を交わすことはほとんど実用性がない。自動的に暗号鍵を共有する方法として，まず公開鍵を共有して，暗号鍵をその公開鍵で暗号化して共有する方法がある。しかし、マン・イン・ザ・ミドル・アタック（Man-in-the-middle attack：マン・イン・ザ・ミドル・アタックの詳細については、ジョン・ウィリィ・アンド・サンズ会社(John Wiley &; Sons, Inc)出版の著者ブルース・シュナイアー（BRUCE SCHNEIER）の題名：応用暗号学（APPLIED CRYPTOGRAPHY）のｐ．４８～ｐ．５０を参照されたい。）のリスクがある。
【０００３】マン・イン・ザ・ミドル・アタックにおけるデータ改ざんのリスクを概略する。図１はアドホック無線通信システム１０において送信元Ａと送信先Ｂとが気付かないままで両者の間に悪意の第三者Ｃが介在する余地を示している。ＡとＢとは、（ａ）のように、両者間に直接、通信路が開設されていると、思っていても、（ｂ）のように、実は第三者が両者の間に割り込んでいる場合がある。"Man-in-the-Middle Attack"がどのように実行されるのか、具体的に例を挙げて説明する。
【０００４】無線暗号通信路開設の一般的な手順は以下のようになる。
手順１：送信元は不特定多数の相手に向かって、通信したい送信先のＩＤで呼びかける。
手順２：送信先が無線接続可能な範囲に居れば、その呼びかけられたＩＤ（つまり自分のＩＤ）を受信する。
手順３：送信先は、自己の動作条件等を送信元に伝える。
手順４：通信路開設のために必要な動作パラメータ（利用する通信路の選択と設定、暗号鍵の交換等）を両者で決定する。
手順５：通信路開設し、相互交信が開始される。
【０００５】悪意の第三者が図１のＣの位置に最も入り込み易いのは、盗聴の対象となる二者が対面で無線通信を開始するタイミングである。つまり、上記の列挙された手順１～３に介入する。図２及び図３は悪意の第三者が図１のＣの位置に入り込む手口の一例を示す。電波の性格上、送信元Ａは周囲のすべての送信先候補に特定ＩＤで呼びかけざるを得ない（手順１）。送信先Ｂは、自分のＩＤでの呼びかけが聞こえるので（手順２）、送信元Ａに応答する（手順３）。ここで、悪意の第三者は自分以外のＩＤへの呼びかけに応答したり、自分以外のＩＤで呼びかけを行ったりして、下記のような成りすましを図ろうとする。まず、悪意の第三者Ｃは送信先Ｂの応答に同一周波数帯のノイズをぶつけて送信元Ａがその応答を聞き取れないようにする。この時点で、送信先Ｂはそのノイズの事実を知らないので、上記手順４に遷移して送信元Ａからの手順４におけるセッション開始を待っている。送信元Ａは手順４には居ないので、送信先Ｂはタイムアウト後に再度、自分のＩＤの呼びかけを聞く状態に戻る。一方、送信元Ａは送信先Ｂからの応答が得られないので、タイムアウト後に再度同じＩＤで呼びかける（手順１）のが普通である。つまり、送信元Ａと送信先Ｂは互いの手順の同期を取り始めようとして、それぞれのタイムアウトでその失敗に気がつき、元の状態に戻ることになる。
【０００６】悪意の第三者Ｃは、送信元Ａが再度同じＩＤで呼びかけるタイミングに合わせて待機し、さらに送信先Ｂが再度自分のＩＤの呼びかけを聞き始めるタイミングにも合わせて待機する。以後、悪意の第三者Ｃは送信元Ａの呼びかけに送信先Ｂに成りすまして応答し、反対に自分のＩＤの呼びかけを聞き始めた送信先Ｂに送信元Ａに成りすまして呼びかけを行う。勿論、悪意の第三者ＣはどのようなＩＤにも自分のＩＤを変化させる能力を用意している。上記で送信元Ａと送信先Ｂが互いの手

順の同期はずれから元の状態に戻るのは同一時刻ではないので、このような二つの成りすまし行為を悪意の第三者Ｃは実行可能である。なぜなら、送信元Ａと送信先Ｂがそれぞれ次のイベントで待機し始める時刻がそもそも異なるし、タイムアウトの対象となるイベントも異なるのでタイムアウト期間自身も異なるからである。

【０００７】この成りすまし工作によって、送信元Ａは、正規の送信先Ｂから正常な応答があったと思って、通信路開設手順、つまり手順４より悪意の第三者Ｃと一緒に遷移するし、送信先Ｂは、正規の送信元Ａからの呼びかけだと思って、通信路開設手順に同じく第三者Ｃと一緒に遷移する。上記手順５まで進むと、二者のみで通信路を確保したと思っている両者Ａ、Ｂの機器の保有者に知られることなく悪意の第三者Ｃが互いの間で通信データを中継する形で盗聴することが可能になる。この成りすまし（中継）を利用すれば、例えばＡがＢに送るはずの公開鍵をＣが改ざんして、Ｃが予め用意した秘密鍵に対応した公開鍵とすり替えることができる。これによって、本来ＡとＢの間で構築される暗号通信路はＡとＣの間でのみ有効になり、ＣとＢとの間はＣが別に設定した暗号通信路となる。つまり、Ａから送られた暗号化データはＣで復号化され、再度ＣとＢの間の暗号化通信路用に別の暗号化を適用されて伝送される。その逆の伝送も同様である。ＡとＢは共に通常手順で暗号化通信路を確立していながら、途中で公開鍵をすり替えられ、そのすり替えに気がつかないことで、盗聴される結果となる。このような攻撃（成りすましによる盗聴）をMan-in-the-middle attackと呼ぶ。暗号化通信路自身は安全であるから、このような攻撃への対処として、通信する両者で本当に同一の公開鍵を共有しているか否かを確実にすることが肝要となる。

【０００８】

【発明が解決しようとする課題】Man-in-the-middle attackの対処法としては、認証機関の発行する証明書を利用して、証明書内に記載された個人ＩＤ（通常相手の名前等）を伝送元、伝送先で表示し目視比較することも考えられる。しかし、これには、証明書の発行にコストがかかる。また、認証機関を利用する場合、身元を登録して認証を行うため、通信相手に自分の身元を公開することになり、匿名性を保つことができないという問題も存在する。さらに、イエローページ（Ｙｅｌｌｏｗ　Ｐａｇｅ）のように公開鍵から利用者を特定するサービスを用いる場合は、電話回線等によるセキュアなネットワーク接続が必要であり、トランザクションコストがかかる。

【０００９】本発明の目的は、アドホック無線接続により相互に接続されるデータ送受装置間でデータを送受する場合において、通信相手へのなりすましによるデータの改ざんを有効に防止できるアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置を提供することである。本発明の他の目的は、口頭やメモ書きによるパスワードの取り交わしを省略でき、身元公開してしまう認証機関を利用せず、能率的に、円滑に、かつ正確に通信相手を検証することのできるアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置を提供することである。

【００１０】

【課題を解決するための手段】本発明のアドホック無線通信用検証システム及び方法によれば、アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【００１１】両データ送受装置の距離は、両データ送受装置の検証データ出力部における検証データを相互に対比する必要があるので、典型的には、両データ送受装置間をユーザ（利用者）が数秒で行き来できる１０m以内等であり、好ましくは数mである。検証データ生成用データに基づいて生成した検証データには検証データ生成用データそのものであってもよいとする。検証データは、両データ送受装置の検出データ出力部における検証データが相互に一致しているか否かの判定が行い易いものに設定される。一般には、両データ送受装置において起動されている検証用ソフトが同一であれば、検証データ生成用データから検証データの生成のために同一の生成アルゴリズムが使用される。しかし、複数個の生成アルゴリズムの内の１個を、両データ送受装置のユーザがその場において適宜、取り決めたりするようになっていてもよい。

【００１２】一方のデータ送受装置は、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて検証データを生成する。他方のデータ送受装置は、受信した検証データ生成用データより第１の生成アルゴリズムに基づいて検証データを生成する。そして、両データ送受装置の検出データ出力部から出力される検証データが一致するか否かの判定を行い、一致していれば、検証データ生成用データが、途中において改ざんされることなく、一方のデータ送受装置から他方のデータ送受装置へ正しく伝送されていること、すなわちデータ完全性

が検証されたことになる。このように、データ完全性の検証を能率的に実施できる。

【００１３】本発明のアドホック無線通信用検証システム及び方法によれば、検証データは、視覚的又は聴覚的な検証データである。

【００１４】視覚的な検証データには、画像、数値、文字、又はそれらの組み合わせがある。検証データの視覚表示の例としては、検証データが例えば計ｎビットのビットデータである場合に、ｎビットを、連続する等ビットずつで区分し、ｘ軸方向へ区分、ｙ軸方向へ各区分ごとの数量とするヒストグラムがある。検証データの聴覚表示の例としては、前述のヒストグラムの各区分の数量に対応する高さの音を、低位の区分から順番に出力するものである。検証データは、両データ送受装置における検証データの一致及び不一致をユーザが円滑かつ正確に判定し易いものが選択されるのが好ましい。

【００１５】本発明のアドホック無線通信用検証システム及び方法によれば、検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていること。

【００１６】検証データの視覚的出力形態では、両データ送受装置におけるもの同士が類似していても、検証データの聴覚的出力形態では相違が明確であり、あるいはその逆の場合がある。検証データの視覚的出力形態及び聴覚的出力形態の両方が対比されることにより、一致及び不一致の判定の正確性が高まる。

【００１７】本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【００１８】一方向性関数には例えばハッシュ関数（Ｈａｓｈ　Ｆｕｎｃｔｉｏｎ）がある。上記定義した演算子列には、演算子が１個しかないものも含んでいる。検証データ生成用データからの検証データの生成に一方向性関数を関与させることにより、検証データから検証データ生成用データを見つけ出す困難性が増大し、悪意の第三者が真の検証データ生成用データに類似の偽の検証データ生成用データを使って、データ改ざんをする可能性が低下する。なお、検証データから検証データ生成用データを見つけ出すことは、直列演算子列の長さが長くなればなる程、計算量的に不可能となる。

【００１９】本発明のアドホック無線通信用検証システム及び方法によれば、第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【００２０】複数個の検証データ全部が類似している可能性は極めて低い。検証データを複数個、生成し、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されることにより、検証の正確性が向上する。

【００２１】本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を２個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された２個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【００２２】本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【００２３】本発明のアドホック無線通信用検証システム及び方法によれば、検証データ生成用データは一方のデータ送受装置の公開鍵である。

【００２４】検証データ生成用データが一方のデータ送受装置の公開鍵であれば、検証データの検証により、他方のデータ送受装置が受信した公開鍵が一方のデータ送受装置の公開鍵であることを検証することができる。したがって、他方のデータ送受装置から一方のデータ送受装置へ一方のデータ送受装置の公開鍵を用いた暗号通信により例えば共通鍵等を送る等して、両データ送受装置間の共通鍵による暗号通信の開設を完全に実施できる。

【００２５】前述のアドホック無線通信用検証システムを利用する本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵Ｋｃを第２

の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２６】前述のアドホック無線通信用検証システムを利用する本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２７】本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Ｋｐから共通鍵Ｋｃを第２の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２８】本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２９】各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとのセキュアな通信路とは、例えば、各ユーザの秘密鍵による相互通信により確立される。無線通信機能付き携帯端末はＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）と呼ばれるものを含む。ビジネスマンの仕事のスタイルの一例としての隠しコンピューティング（Ｈｉｄｄｅｎ　Ｃｏｍｐｕｔｉｎｇ：発明の実施の形態において詳述）が考えられている。隠しコンピューティングでは、例えばノートＰＣ等の無線通信機能付きパソコン同士で、改ざんなくデータの送受が行われることが望まれる。このようなケースにおいて、ユーザは無線通信機能付き携帯端末の検証データ出力部における検証データの対比から一方の無線通信機能付き携帯端末の公開鍵Ｋｐが途中に改ざんされることなく他方の無線通信機能付き携帯端末へ伝送されたことが検証されると、その検証を両ユーザの無線通信機能付きパソコンへ引き継がせ、両無線通信機能付きパソコンの間で共通鍵Ｋｃにより暗号通信を円滑に実施できる。

【００３０】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものである。

：アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【００３１】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。録媒体。

：検証データは、視覚的又は聴覚的な検証データである。

【００３２】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに

付加される。
：検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっている。
【００３３】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。
：関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。
【００３４】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。
：第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。
【００３５】
【発明の実施の形態】以下、発明の実施の形態について図面を参照して説明する。図４はデータ完全性の検証及びそれに続く暗号データ伝送の全体のフローチャートである。暗号通信開設要求側及び被要求側をそれぞれ伝送元及び伝送先と定義し、図４では、伝送元データ送受装置をＡ、伝送先データ送受装置をＢとしている。データ完全性検証のための公開鍵の伝送元及び伝送先と、データ完全性検証後の本伝送（ほんでんそう：共通鍵を使った暗号伝送）の伝送元及び伝送先とは、一致している必要はなく、逆であってもよいし、また、データ完全性検証後の本伝送では、伝送元及び伝送先は適宜、入れ替わってもよい。
【００３６】図４の処理を順番に説明する。
（ａ）Ａは、Ｂに暗号通信路開設要求と共に自分の公開鍵Ｋｐ、及び検証データ生成アルゴリズムを指定するＩＤ（以下、このＩＤを「ＩＤ１」と言う。）を送信する。Ａは、同時に、自分の公開鍵Ｋｐを元に検証データＸｐを生成する。
（ｂ）ＢがＡからＡの公開鍵Ｋｐとして受信したデータをＫｘとする。もし、ＡからＢへの無線伝送路においてデータの改ざんがなければ、Ｋｘ＝Ｋｐとなり、改ざんがあれば、ＫｘはＫｐとは別のものとなる。ＢはＡから受け取ったＫｘを元に、Ａより指定のあったＩＤ１の検証データ生成アルゴリズムで検証データＸｘを生成する。検証データの例は、後述の図５において詳述する。
（ｃ）Ａ、Ｂのユーザは、Ａ及びＢの表示部にそれぞれ出力表示された検証データＸｐ，Ｘｘが同一であるか否かを検証する。もし、Ｘｐ＝Ｘｘであれば、Ｋｘ＝Ｋｐを意味し、Ａ－Ｂの通信路にはデータ完全性があるとの判断を下す。
（ｄ）ＢはＡから受信した公開鍵Ｋｐを使って、共通鍵生成のための乱数値Ｒと共通鍵生成アルゴリズムを指定するＩＤ（以下、このＩＤを「ＩＤ２」と言う。）とを暗号化して、Ａへ送信する。ＩＤ２については、Ａ，Ｂが同一の通信ソフトを使用する等、ＩＤ２が固定されているならば、ＩＤ１と同様に、Ａ－Ｂ間の伝送は省略できる。Ｂは、同時に乱数値Ｒから共通鍵生成アルゴリズムを用いて共通鍵Ｋｃを生成する。
（ｅ）ＡはＢから受信した暗号化された乱数値Ｒを、公開鍵Ｋｐに対応する秘密鍵を使って復号し、乱数値ＲとＩＤ２とを得、乱数値ＲからＩＤ２の共通鍵生成アルゴリズムを用いて共通鍵Ｋｃを生成する。
（ｆ）以降、Ａ－Ｂは、共通鍵Ｋｃに基づく暗号化通信によりデータを送受する。
【００３７】Ａ，Ｂの検証データ出力部に表示する検証データは検証データ生成用データそのもの、例えばＡの公開鍵そのものであってもよい。すなわち、Ａ，Ｂの検証データ生成用データに、Ａの公開鍵がビット表示される。しかし、数値では、読み取り難いので、公開鍵の数値表示を画像表示へ変換してもよい。 図５は検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す。検証データはデータ送受装置２０（図６）の検証画像表示部２７に視覚表示される。検証データ生成用データがＡの公開鍵であるとして、公開鍵をＬＳＢからＭＳＢまでを等しいビット数の区域に順番に区切り、横軸を区域、縦軸を各区域の数量とするヒストグラムで、検証データが表されている。もし、Ａの公開鍵Ｋｐが、伝送路の途中で悪意の第三者により成りすましが行われていなければ、ＢがＡより受信した検証データ生成用データＫｘは、検証データ生成用データＫｐに等しいので、Ｘｘ＝Ｘｐとなる。したがって、Ａ及び／又はＢのユーザ、又は信頼できる他の検証者は、Ａ，Ｂの表示部を直接、見て、Ａ，Ｂの表示部に表示されているＸｐ及びＸｘを対比（比較）し、両者が一致していれば、ＡからＢへＡの公開鍵がそのまま伝送されて来たと判断し、すなわちデータ完全性があると判断し、両者が不一致であれば、ＡからＢへの伝送途中にデータの改ざんがあったと判断する。
【００３８】しかし、人間の認識能力の精度は必ずしも高くなく、図５のようなヒストグラムの比較画像を単純に生成しただけではハミングディスタンスの小さい類似公開鍵との違いを検出できない場合がある。そこで、公開鍵に対してハッシュ関数等の一方向性関数を適用して所定のデータへ変換し、それをヒストグラム等の検証画像の表示を行ってもよい。この場合、成りすましを行おうとする第三者が類似するデータを出力する別の公開鍵を求めようとしても、離散対数問題を解くことになり計算量的に不可能である。ただし、作成する検証画像の情報量が公開鍵のビットサイズに比べて極めて小さい場合、全数探索によって破られる可能性がある。そのよう

な条件下では、すでに一方向性関数を適用したデータに対してさらに一方向性関数を適用して新たなデータを算出したり、別の一方向性関数を公開鍵に適用して新たなデータを算出したりして、別の検証画像を生成する。この操作を繰り返すことで、複数の検証画像を生成することができ、これを用いることで成りすましに対する強度をあげることができる。

【００３９】検証データは、ヒストグラムのような画像に限定されず、文字データの表示や音階の変化などを用いたり、それらの複数のデータを組み合わせたりして、ユーザに対して提示したりしてもよい。聴覚的な検証データとしては、図５のヒストグラムの縦軸方向の値を音の高低又は音色に対応させ、図６の横軸方向の左の区域から順番に所定時間ごとに各区域の値に対応する音を出力する。また、検証データを視覚表示器と放音手段としてのスピーカとの両方から出力させるようにしてもよい。

【００４０】図６～図８は一方向性関数を使用して検証データ生成用データから検証データを生成する方式をそれぞれ示している。データＤ１は検証データ生成用データを意味し、データＤ２，Ｄ３，Ｄ４，・・・は検証データを意味する。また、各一方向性関数は、演算子として機能し、入力に作用して、演算結果を出力する。一方向性関数は例えばハッシュ関数（Ｈａｓｈ　Ｆｕｎｃｔｉｏｎ）である。

【００４１】図６では、１回目は検証データ生成用データとしてのデータＤ１に一方向性関数Ｆを作用させ、データＤ２を得る。２回目は、データＤ２に同一の一方向性関数Ｆを作用させ、すなわち、一方向性関数Ｆを含むループを形成し、データＤ３を得る。以降、ループ処理を繰り返し、Ｄ４、Ｄ５、・・・を得る。所定回数のループを繰り返した後、最終的な演算結果をＤｎとし、このＤｎを検証データとし、この検証データをデータ送受装置２０（図１０）の検証画像表示部２７に視覚表示する。最終的な演算結果Ｄｎのみデータ送受装置２０の検証画像表示部２７に視覚表示するだけでなく、Ｄ２，Ｄ３，Ｄ４，・・・の特定の幾つか又は全部をデータ送受装置２０の検証画像表示部２７に画面分割又は時分割で視覚表示させることにし、表示されたそれぞれについて対比してもよい。複数の検証データを対比することにより、たとえそれらの１個の検証データについての一致・不一致の判定が紛らわしくても、対比される複数の検証データのすべてについて一致・不一致の判定が紛らわしくなる可能性は極めて小さく、データ改ざんについての検証の正確性を向上できる。

【００４２】なお、Ｄ２，Ｄ３，Ｄ４，・・・の全部でなく、特定の幾つかのみを対比する場合に、その幾つかについての組み合わせ（Ｓｕｂｓｅｔ）を適宜、変更するようにしておくことにより、悪意の第三者の攻撃に対する防護強度は高くなる。

【００４３】図７では、相互に異なる複数個の一方向性関数Ｆ，Ｇ，Ｈ，・・・を用意し、共通のデータＤ１に各一方向性関数Ｆ，Ｇ，Ｈ，・・・を作用させ、各演算結果Ｄ２，Ｄ３，Ｄ４，・・・を得る。Ｄ２，Ｄ３，Ｄ４，・・・の特定の幾つか又は全部を検証データとして、データ送受装置２０の検証画像表示部２７に画面分割又は時分割で視覚表示させ、表示されたそれぞれについて対比する。

【００４４】図８では、相互に異なる複数個の一方向性関数Ｆ，Ｇ，Ｈ，・・・を用意する。１回目は検証データ生成用データとしてのデータＤ１に一方向性関数Ｆを作用させ、データＤ２を得る。２回目は、データＤ２に一方向性関数Ｇを作用させ、データＤ３を得る。こうして、次々に前段の演算結果に次段の一方向性関数を作用させ、複数個のＤ２，Ｄ３，Ｄ４，・・・を得る。Ｄ２，Ｄ３，Ｄ４，・・・の特定の幾つか又は全部を検証データとして、データ送受装置２０の検証画像表示部２７に画面分割又は時分割で視覚表示させ、表示されたそれぞれについて対比する。なお、図６における複数個対比の方式は、図８の方式において、相互に異なる一方向性関数を使用する代わりに同一の一方向性関数Ｆを使用した特殊の例と考えることができる。

【００４５】図９は図６～図８の処理を組み合わせて検証データを求める方式を示すブロック図である。図６～図９の検証データ演算方式をそれぞれタイプ（Ｔｙｐｅ）１，２，３と定義している。図８の左端に検証データ生成用データが入力され、図８の右端に検証データが出力される。図９の配列例は一例である、タイプ１，２，３から２個以上のタイプを選択し、それらを任意の順に並べて、検証データ生成用データを得ることができる。

【００４６】図１０はデータ送受装置２０のブロック図である。データ送受装置２０は、場合により伝送元Ａになったり、伝送先Ｂになったするので、伝送元としての構成と伝送先としての構成を兼備している。データ送受装置２０がＡである場合には、伝送検証部２４は、自分の公開鍵を検証画像生成部２６へ出力し、また、データ送受装置２０がＢである場合には、通信部２５においてＡからの送受信データ３１として受信したＡの公開鍵は伝送検証部２４を経由して検証画像生成部２６へ送られる。検証画像生成部２６は伝送検証部２４から受けた公開鍵から検証データを生成し、生成された検証データは検証画像表示部２７に表示される。Ａ，Ｂの所有者等のユーザは、アドホック無線接続されている２個のデータ送受装置２０の検証画像表示部２７における検証データを対比し、一致及び不一致を調べ、その結果を検証結果入力部２８に入力する。ユーザからの検証結果入力部２８への入力結果は伝送検証部２４へ通知され、伝送検証部２４は、両検証データが相互に一致しているとの通知を受けた場合には、ＡからＢへアドホック無線接続の伝

送路を介して伝送した公開鍵についてデータ完全性があると判断する。次に、データ送受装置２０がＢである場合には、乱数生成部３４において乱数値が生成され、共通鍵生成部３３では、乱数生成部３４において生成された乱数値からＩＤ２の共通鍵生成アルゴリズムにより共通鍵を生成する。一方、乱数生成部３４が生成した乱数値及びＩＤ２が復号化・暗号化実施部３２においてＡの公開鍵に基づいて暗号化され、その暗号データＤｃが送受信データ３１を介してＡへ送られる。また、乱数値ＲからＩＤ２の生成アルゴリズムに基づいて共通鍵を生成し、それを鍵保存部３５に保存する。データ送受装置２０がＡである場合には、Ｂから伝送されて来た暗号データＤｃの送受信データ３１を復号化・暗号化実施部３２において自分の秘密鍵により復号し、乱数値Ｒ及びＩＤ２を得、乱数値ＲからＩＤ２の共通鍵生成アルゴリズムに基づいて共通鍵を生成し、該共通鍵を鍵保存部３５に保存する。以降は、データを送信する場合は、鍵保存部３５から共通鍵を引き出して、該共通鍵に基づいて送信データを復号化・暗号化実施部３２において暗号化し、送受信データ３１として相手方へ送信する。データを受信する場合は、受信した暗号化され送受信データ３１を復号化・暗号化実施部３２において復号し、平データをハードディスク（図示せず）等に保存したり、所定の処理を行ったりする。

【００４７】図１１は伝送元Ａ側の通信処理のフローチャートである。公開鍵Ｋｐを送信し（Ｓ４０）、該公開鍵ＫｐからＩＤ１の検証データ生成アルゴリズムにより検証データＸｐを生成し（Ｓ４２）、検証データＸｐを検証画像表示部２７に出力する（Ｓ４４）。Ｓ４６では、自分の検証データＸｐと伝送先Ｂの検証データＸｘとを対比して、同一と判断されれば、Ｓ４８へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、伝送先Ｂからの乱数値Ｒの受信を待ち（Ｓ４８）、Ｓ５０において、乱数値Ｒを受信したと判断すると、Ｓ５２へ進み、乱数値受信待ち時間が所定時間経過したにもかかわらず、乱数値Ｒの受信のないときは、エラーとして該プログラムを終了する。Ｓ５２では、伝送先Ｂからの乱数値Ｒの暗号データを前記公開鍵Ｋｐに対応の自分の秘密鍵で復号して、乱数値Ｒを得る。Ａ，Ｂのデータ送受装置間では複数個の共通鍵生成アルゴリズムについてそれぞれＩＤが予め取り決められており、送信先Ｂにおいて今回の共通鍵生成アルゴリズムとして採用されたＩＤ（例では、ＩＤ２）が乱数値Ｒと一緒に伝送先Ｂから伝送元Ａへ送信されて来ている。こうして、Ｓ５６では、乱数値ＲからＩＤ２の共通鍵生成アルゴリズムに基づいて送信先Ｂとの通信用の共通鍵を生成し、以降、該共通鍵を用いてＢと暗号化通信を開始する（Ｓ５８）。

【００４８】図１２は伝送先Ｂ側の通信処理のフローチャートである。伝送元Ａから公開鍵Ｋｘを受信する（Ｓ６０）。この受信した公開鍵は、Ａ，Ｂ間の伝送路に悪意の第三者が介在していて改ざんされている可能性があるかもしれないので、Ｋｃではなく、Ｋｘと表現することにする。次に、送信元Ａから公開鍵Ｋｐと一緒に送られて来たＩＤ１で指定される検証データ生成アルゴリズムによりＫｘから検証データＸｘを生成し（Ｓ６２）、検証データＸｘを検証画像表示部２７に出力する（Ｓ６４）。Ｓ６６では、自分の検証データＸｘと伝送元Ａの検証データＸｐとを対比して、同一と判断されれば、Ｓ６８へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、乱数値Ｒを生成し（Ｓ６８）、乱数値Ｒと、複数個の共通鍵生成アルゴリズムの中から、今回、選択した共通鍵生成アルゴリズムのＩＤとしてのＩＤ２とを送信元Ａの公開鍵により暗号化したデータを送信元Ａへ送信し（Ｓ７０）、ＩＤ２の共通鍵生成アルゴリズムに従って共通鍵Ｋｃを生成し（Ｓ７２）、以降、該共通鍵を用いてＡと暗号化通信を開始する（Ｓ７４）。

【００４９】図１３は隠れコンピューティングスタイルの利用するユーザ間においてアドホック無線接続の暗号通信路を開設する説明図である。隠れコンピューティング（Hidden Computing）とは、ユーザは、コンピュータを鞄等に納め、手元のＰＤＡ（携帯情報端末：Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等の携帯機器から無線通信等を利用して該コンピュータを遠隔操作する利用形態を意味する。ＰＤＡ８０ａ等に装備されている８２は通信デバイスである。上記に述べたような公開鍵のデータの完全性を確認できるシステムを装備していない機器（＝鞄８６ａ，８６ｂの中のノートパソコン８８ａ，８８ｂ）間でアドホック無線通信を行う場合において、これらノートパソコン８８ａ，８８ｂと事前にセキュアな通信路９０ａ，９０ｂを確保している暗号通信路開設プロトコルを実装したＰＤＡ８０ａ，８０ｂを用いて、間接的に暗号通信路を開設する。なお、ＰＤＡとノートパソコンとの間のセキュアな通信路は、例えば両者間で事前に取り決められている共通鍵による暗号通信により達成される。図１３においてまず手順（ａ）で通信路８４をＰＤＡ８０ａ，８０ｂ間で開設して、一方のＰＤＡの公開鍵を他方のＰＤＡへ伝送して、該公開鍵のデータ完全性を検証する。次に、手順（ｂ）においてＰＤＡ８０ａ，８０ｂ間のデータ完全性検証を、それぞれのＰＤＡ８０ａ，８０ｂとセキュアな通信路９０ａ，９０ｂにより接続されているノートパソコン８８ａ，８８ｂへ継承する。この継承は、具体的には、ＰＤＡ８０ａ，８０ｂ間でデータ完全性を検証された公開鍵をセキュアな通信路９０ａ，９０ｂを介してノートパソコン８８ａ，８８ｂを伝送することにより達成される。以降、ノートパソコン８８ａ，８８ｂは、両者間の

通信路９２を介して共通鍵を共有した後、該共通鍵による暗号でデータを送受する。

【図面の簡単な説明】

【図１】送信元Ａと送信先Ｂとが気付かないままで両者の間に悪意の第三者Ｃが介在する余地を示す図である。

【図２】悪意の第三者が図１のＣの位置に入り込む手口の一例の第１の部分を示す図である。

【図３】悪意の第三者が図１のＣの位置に入り込む手口の一例の第２の部分を示す図である。

【図４】データ完全性の検証及びそれに続く暗号データ伝送の全体のフローチャートである。

【図５】検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す図である。

【図６】一方向性関数を使用して検証データ生成用データから検証データを生成する第１の方式を示す図である。

【図７】一方向性関数を使用して検証データ生成用データから検証データを生成する第２の方式を示す図である。

【図８】一方向性関数を使用して検証データ生成用データから検証データを生成する第３の方式を示す図である。

【図９】図６～図８の処理を組み合わせて検証データを求める方式を示すブロック図である。

【図１０】データ送受装置のブロック図である。

【図１１】伝送元Ａ側の通信処理のフローチャートである。

【図１２】伝送先Ｂ側の通信処理のフローチャートである。

【図１３】隠れコンピューティングスタイルの利用するユーザ間においてアドホック無線接続の暗号通信路を開設する説明図である。

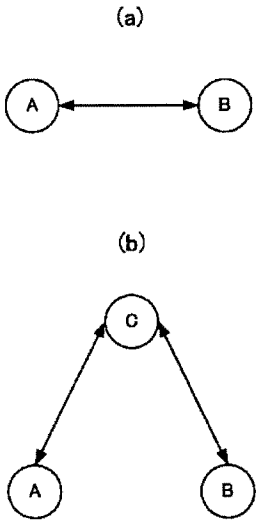
【符号の説明】

１０　　アドホック無線通信システム

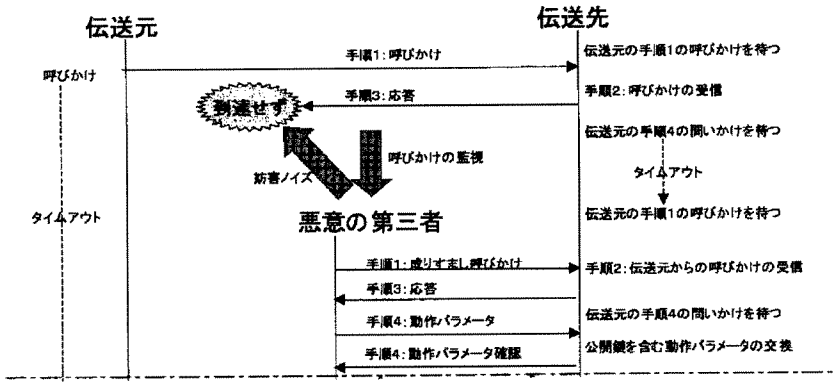
８０ａ，８０ｂ　　ＰＤＡ（無線通信機能付き携帯情報端末）

８８ａ，８８ｂ　　ノートパソコン（無線通信機能付きパソコン）

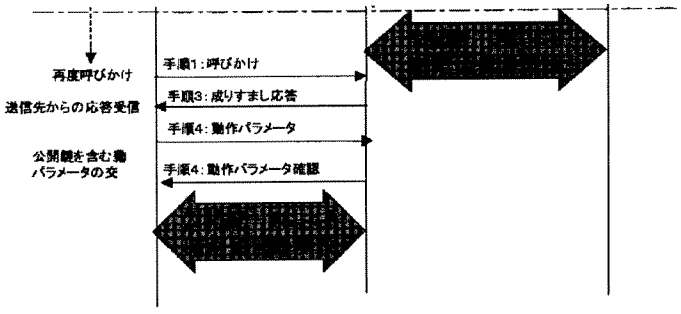
【図１】



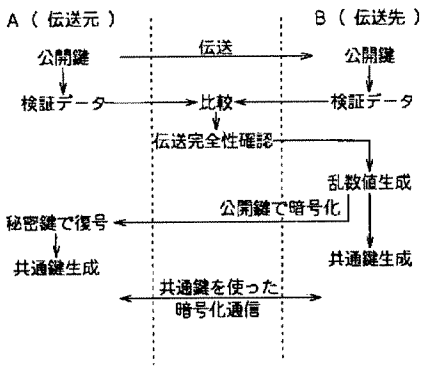
【図２】



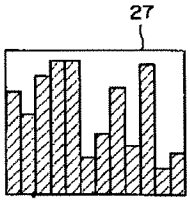
【図３】



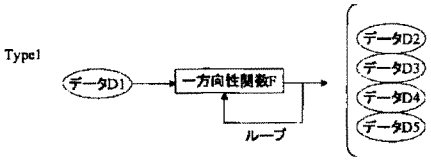
【図４】



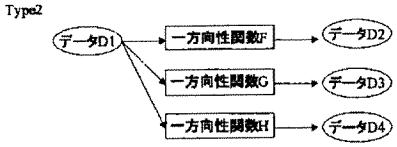
【図５】



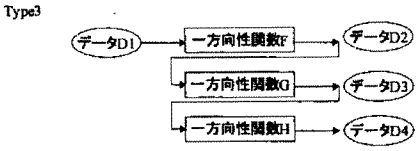
【図６】



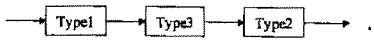
【図７】



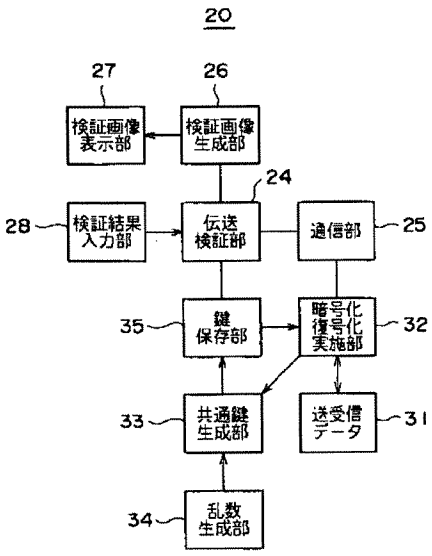
【図８】



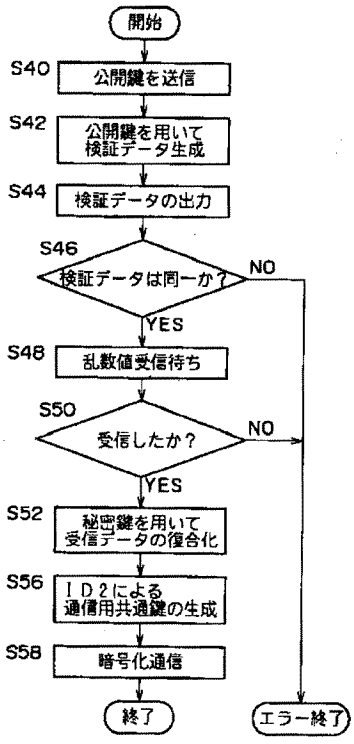
【図９】



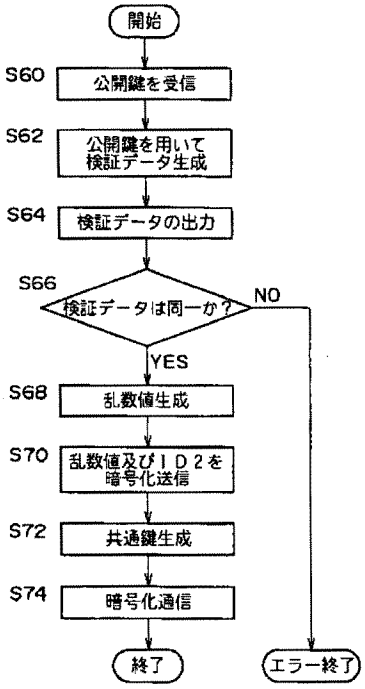
【図１０】



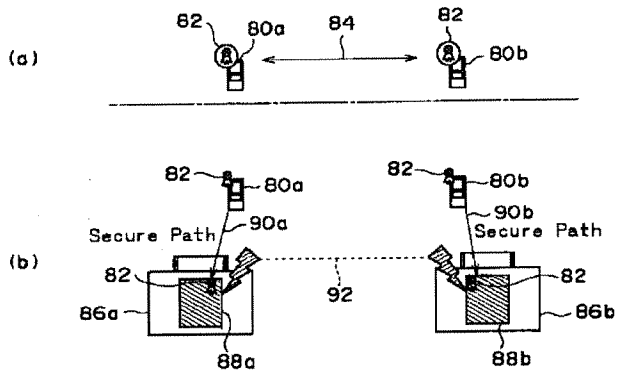
【図１１】



【図１２】



【図１３】



フロントページの続き

(51) Int. Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ（参考）
		Ｈ０４Ｌ　11/00	３１０Ｂ

(72)発明者　野口　哲也
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内
(72)発明者　下遠野　享
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

Ｆターム(参考)　5J104 AA07 AA08 AA16 AA41 EA04
EA10 EA19 JA21 JA29 KA01
KA05 LA01 NA02 NA11 NA12
NA24
5K033 AA08 BA08 DA17 DB20
5K067 AA33 BB04 BB21 DD17 DD53
EE02 EE10 EE16 FF23 FF25
HH22 HH23 HH36